

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK  
WHITE PLAINS DIVISION**

JENNIFER WEDEKING, on behalf of herself and  
all others similarly situated,

Plaintiff,

v.

INTERNATIONAL BUSINESS MACHINES  
CORPORATION,

Defendant.

Case No. \_\_\_\_\_

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

## **CLASS ACTION COMPLAINT**

Plaintiff Jennifer Wedeking (the “Plaintiff”), on behalf of herself and all others similarly situated, alleges the following Class Action Complaint (the “Action”) against the above-captioned Defendant, International Business Machines Corporation (“IBM” or “Defendant”) upon personal knowledge as to herself and her own actions, and upon information and belief, including the investigation of counsel as follows:

### **I. NATURE OF THE ACTION**

1. For millions of unsuspecting victims, Defendant IBM critically failed to properly secure and safeguard personally identifiable information (“PII”), including but not limited to: Plaintiff’s and the Class members’ name, Social Security number, Medicaid ID number, Medicare ID number, date of birth, home address and contact information, demographic or income information, clinical and medical information (including diagnosis/condition, lab results, medication, or other treatment information), and health insurance information.

2. Defendant is a substantial technology services corporation with the knowledge, expertise and resources to take seriously the obligation to protect private information. However, IBM apparently made a conscious decision not to invest the time or resources necessary to protect the PII of Plaintiff and the Class members.

3. On behalf of a number of its corporate and governmental-entity clients, IBM collects or maintains a significant amount of private information, including the PII listed above. In the conduct of this business, IBM contracts with software companies to provide the necessary technological resources to transfer and store said PII. An example of this includes an entity known as PSC, a software company, hired by IBM on behalf of the Colorado Department of Health Care Policy and Financing’s (“HCPF”) for the storage and transfer of data entrusted to IBM.

Specifically, IBM uses PSC's MOVEit transfer file services for a variety of purposes, including the transfer of Plaintiff's and the Class members' PII.

4. Like millions of Americans who had their PII stored by various business and governmental entities around the country, Plaintiff's and the Class members' PII was given to IBM for such purposes and was, in turn, entrusted by IBM to PSC. In undertaking this responsibility, IBM was obligated to only hire vendors who maintain adequate data security practices. However, due to a crucial vulnerability in PSC's MOVEit software, the inadequately protected PII of millions of victims entrusted to IBM was compromised. To take merely one example, nearly 4.1 million Coloradans whose PII was given to IBM by HCPF were affected. This Action seeks to represent victims of every organization whose PII was compromised due to IBM's negligent conduct in hiring and monitoring PSC.

5. According to the Notice of Data Breach received by Plaintiff, which was received not from Defendant IBM but from HCPF, on or around May 31, 2023, PSC disclosed a major vulnerability that had been exploited by an unauthorized cybercriminal. Over the course of investigating, HCPF discovered that, on May 28, 2023, third-party cybercriminals not only exploited the MOVEit software, but downloaded and exported the data of Plaintiff and other Class members. This was just one organization of many that entrusted PII to IBM. IBM failed to protect that data and, instead, allowed that PII to be compromised when PSC's MOVEit software was breached (the "Data Breach"). This Data Breach was likely perpetrated by a well-known cybergang called Cl0p. The *modus operandi* of a cybergang like Cl0p is to offer for sale (on the dark web) unencrypted, unredacted private information like the PII of Plaintiff and the Class members. Thus, the Plaintiff and the Class members are in imminent harm of identity theft and other identity-related crimes.

6. To compound matters, IBM never even informed Plaintiff directly of the harm she suffered due to the Data Breach. For its part, in the case of HCPF, HCPF did not disclose the Data Breach to victims until August 11, 2023 – nearly ten full weeks after the Data Breach was first discovered on May 31, 2023; and the Notice of Data Breach failed to disclose the specifics of the cyberattack (*i.e.*, how it happened) as well as specific remedial measures taken to ensure the protection of the PII still in HCPF’s and the Defendant’s possession. Further, the only remediation here was not even offered by IBM: a meager 24 months of identity theft protection for victims of the Data Breach when the impact of the theft of this sort of PII set at-issue will ripple for many years, if not decades. While IBM could have given Plaintiff and the Class members the ability to start taking action (like imposing credit freezes) to protect themselves, IBM continues to make a conscious decision not to do so.

7. Notably, the Data Breach response was worsened too by the fact that, in the case of HCPF, HCPF was the issuer of the Notice of Data Breach, a governmental agency that many Class members never heard of. Undoubtedly, this led to Class members discarding the Notice of Data Breach. Hence, to this day, the vast majority of those Class members have no knowledge that they are even victims. IBM, as the party that hired PSC, should have been the entity responsible for the distribution of said notices.

8. IBM negligently chose to utilize PSC’s MOVEit search services with Plaintiff’s and the Class members’ PII even though the MOVEit software contained significant security vulnerabilities. The potential for this Data Breach was a known risk to IBM because of other file transfer programs that had been previous subjected to criminal hacking, and, thus, IBM was on notice that failing to take appropriate design and protective measures would expose and increase the risk that PII would be compromised and stolen.

9. As such, Plaintiff, on behalf of herself and all others similarly situated, brings this Action for restitution, actual damages, nominal damages, statutory damages, injunctive relief, disgorgement of profits and all other relief that this Court may deem just and proper.

## **II. JURISDICTION AND VENUE**

10. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d). The amount of controversy exceeds the sum of \$5,000,000 exclusive of interests and costs, there are more than 100 putative Class members, and minimal diversity exists because one or more putative Class members are citizens of a different state than Defendant.

11. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in Armonk, New York. Furthermore, Defendant intentionally availed itself of this jurisdiction by marketing, employing individuals, and providing technology services in New York.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant operates in this District and a substantial part of the events, acts and omissions giving rise to Plaintiff’s claims occurred in this District.

## **III. PARTIES**

### ***Plaintiff Jennifer Wedeking***

13. Plaintiff Jennifer Wedeking is, and at all times mentioned herein was, a citizen of the state of Colorado. Plaintiff Wedeking received a copy of the Notice of Data Breach disseminated by HCPF.

14. As a result of Defendant’s failure to protect Plaintiff Wedeking’s PII, Plaintiff Wedeking’s PII has been compromised in the Data Breach.

***Defendant IBM***

15. IBM is domiciled and maintains its principal place of business in the State of New York.

16. IBM offers technology-based solutions to consumers and businesses, including HCPF for example, throughout the United States.

17. According to the Notice of Data Breach received by Plaintiff, IBM hired PSC. MOVEit file transfer is a product of PSC. PSC is a third-party software vendor that offers a wide range of products and services to government agencies and corporate entities around the world, including MOVEit. MOVEit is a “[m]anaged file transfer and automatic software that guarantees the security of sensitive files both at-risk and in-transit, ensures reliable business processes and addresses data security compliance requirements.”

**IV. FACTUAL ALLEGATIONS**

***The Collection of Private Information***

18. In the course of doing business, IBM acquires and maintains a significant amount of highly valuable private information from constituent consumers, including the acquisition of the PII of Plaintiff and the Class members.

19. According to the Notice of Data Breach received by Plaintiff, IBM was to provide various technology-related functions. In the process of doing this, IBM acquired a significant amount of constituent consumers’ private information, including the PII of Plaintiff and the Class members. To store and transfer said PII, IBM decided to (and did) use PSC’s MOVEit file storage and transfer system.

20. As a condition of providing their PII, Plaintiff and the Class members entrusted that the organizations to which they furnished their PII would only use their data for business purposes

in a way that was safe and secure, which includes and extends to the hiring of any third-party vendors, such as IBM.

21. By obtaining, collecting, using, and deriving a benefit from Plaintiff and the Class members PII, IBM assumed legal and equitable duties and knew that it was responsible for ensuring the security and safety of Plaintiff and the Class members' PII to protect it from unauthorized disclosure and exfiltration.

22. Plaintiff and the Class members relied on IBM to keep PII confidential and security maintained, and only to make authorized disclosures of this information, which IBM failed to do.

***The Data Breach***

23. On May 31, 2023, PSC reported a vulnerability in MOVEit Transfer and MOVEit Cloud that could lead to escalated privileges and potential unauthorized access to the data environment. PSC purportedly launched an investigation, alerted MOVEit customers, including IBM, of the issue and provided mitigation steps.

24. This was confirmed by HCPF in the Notice of Data Breach it furnished to Plaintiff. According to the Notice of Data Breach:

**What Happened?** On May 31, 2023, [PSC] discovered a problem affecting its MOVEit Transfer application. IBM a third-party vendor contracted with HCPF uses the MOVEit application to move HCPF files in the normal course of business.

...

After IBM notified HCPF that it was impacted by the MOVEit incident, HCPF launched an investigation right away to understand whether the incident impacted our own systems... While we confirmed that no other HCPF systems or databases were impacted, on June 13, 2023, the investigation identified that certain HCPF files were accessed by [an] unauthorized actor on or about May 28, 2023.

...

**What Information Was Involved?** The information compromised may have included one or more of the following pieces of information: your full name, Social

Security number, Medicaid ID number, Medicare ID number, date of birth, home address and other contact information, demographic or income information, clinical and medical information (such as diagnosis/condition, lab results, medication, or other treatment information), and health insurance information.

25. Plaintiff and the Class members have to contend with the harm that the Data Breach caused.

26. First, IBM to this day has not informed Plaintiff about the Data Breach. In fact, no one disclosed this Data Breach to victims until August 11, 2023, ten full weeks after IBM first became aware of it. That means that, for nearly ten weeks, IBM could have alerted victims to the fact that their PII was compromised but failed to do so. Instead, IBM chose to sit on that information and allow valuable time to pass while Plaintiff and the Class members suffered the harms discussed herein.

27. Second, IBM has offered the victims nothing. In the case of HCPF, which was not the victim of the data breach itself, HCPF has offered victims an insufficient 24 months of identity theft monitoring services when the impact of the theft of the PII at-issue ripples for decades. Although it is well-documented that the harms from identity theft can affect a person for a lifetime, IBM refuses to provide the victims of the Data Breach with adequate protection.

28. Finally, the disclosure itself was inadequate. The Notice of Data Breach received by Plaintiff did not disclose the specifics of the cyberattack or the specific remedial measures being taken to ensure the protection of the PII still in IBM's (and other third-party vendors') possession. All of this information remains unclear to the victims of the Data Breach.

29. What is clear, however, is that cybercriminals did download and exfiltrate the PII of Plaintiff and the Class members.



30. On information and belief, the PII compromised in the files accessed by hackers was not encrypted. This can also be inferred given that Clop was able to access the data that was listed as compromised in the Notice of Data Breach received by Plaintiff.

31. Armed with this PII, data thieves, like Clop (as well as downstream purchasers of the stolen PII), can commit a variety of crimes, including: opening new financial accounts in Class members' names, taking out loans in Class members' names, using Class members' information to obtain government benefits, filing fraudulent tax returns using Class members' tax identification information, obtaining driver's licenses in Class members' names but with a different photograph, and giving false information to police during an arrest.

32. Due to IBM's incompetent response to the Data Breach, Plaintiff and the Class members now face a present and substantial risk of fraud and identity theft and must deal with that threat forever.

33. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks and unauthorized disclosure of PII, IBM provided unreasonably deficient protections prior to the Data Breach, including but not limited to a lack of security measures for storing and handling PII and inadequate employee training regarding how to access, oversee the protection, handle and safeguard for this sensitive set of information.

34. IBM's failures caused the unpermitted disclosure of Plaintiff's and the Class members' PII to an unauthorized third-party cybercriminal and put Plaintiff and the Class members at serious, immediate, and continuous risk of identity theft and fraud.

35. The Data Breach that exposed Plaintiff's and the Class members' PII was caused by IBM's failure to abide by best practices and industry standards concerning its information security practices and processes, and its use of third parties such as PSC.

36. IBM failed to comply with basic security standards or to implement security measures that could have prevented or mitigated the Data Breach. Additionally, IBM failed to properly select its third-party information security partners, ensure the proper monitoring and logging of the ingress and egress of data and network traffic, ensure the proper training of its and its technology partners' employees as to best practices, disclose the Data Breach in a timely manner, and disclose the potential vulnerabilities in its cybersecurity apparatus prior to the collection of PII.

***The Breach Was Foreseeable***

37. IBM has significant obligations created by industry standards, common law, and its own promises and representations to keep PII confidential and to protect it from unauthorized access and disclosure.

38. Plaintiff and the Class members provided their PII to various corporate and governmental entities (such as HCPF) with the reasonable expectation and mutual understanding that third-party vendors such as IBM would comply with its obligations to keep such information confidential and secure from unauthorized access.

39. IBM's data security obligations were particularly acute given the substantial increase in ransomware attacks and/or data breaches in various industries preceding the date of the Data Breach.

40. IBM is aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

41. Cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

42. PII is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners. PII can be used to distinguish, identify or trace an individual's identity. This can be accomplished alone or in combination with other personal or identifying information that is connected or linked to an individual, such as the information compromised in the Data Breach.

43. Given the nature of the Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of different ways.

44. Cybercriminals who possess the Class members' PII can readily obtain Class members' tax returns or open fraudulent credit card or other types of accounts in the Class members' names.

45. The increase in such attacks, and attendant risk of future attacks, was widely known.

46. As such, this specific Data Breach was foreseeable.

***IBM Failed to Follow FTC Guidelines, HIPAA and Industry Standards***

47. Government agencies highlight the importance of cybersecurity practices. For example, the Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

48. According to the FTC, the need for data security should be factored into all business decision-making.

49. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

50. The guidelines note that companies that maintain PII should protect the personal information that they keep; properly dispose of personal information that is no longer needed;

encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

51. The guidelines also recommend that companies that maintain PII use an intrusion detection system to detect and expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

52. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

53. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, in some cases treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further explicate and clarify the measures businesses must take to meet their data security obligations.

54. IBM failed to properly implement some or all of these (and other) basic data security practices.

55. IBM's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

56. Additionally, IBM (as a third-party vendor for various entities) maintains data related to healthcare services and health insurance for consumers, like Plaintiff and the Class members, and is therefore subject to the Health Insurance Portability and Accountability Act (“HIPAA”). IBM was thus subject to the requirements of HIPAA, as well as the HIPAA’s various privacy rules and other related regulations. HIPAA requires numerous safeguards to protect private information with which IBM apparently did not comply, including oversight and monitoring of the data that it controls, overseeing service providers and requiring them by contract to protect the security and confidentiality of consumer information.

57. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

58. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of Protected Health Information (“PHI”). Safeguards must include physical, technical, and administrative components.

59. Title II of HIPAA contains what are known as the Administrative Simplification provisions. These provisions require, among other things, that the Department of Health and Human Services (“HHS”) create rules to streamline the standards for handling PHI and PII like the data Defendant left unsecured.

60. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA.

61. A data breach such as the one at issue, is also considered a breach under the HIPAA Rules because there is access of PHI not permitted under the HIPAA Privacy Rule: A breach under the HIPAA Rules is defined as “...the acquisition, access, use, or disclosure of PHI in a manner

not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.” *See* 45 C.F.R. 164.40.

62. Data breaches are “Security Incidents” under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information: the presence of ransomware (or any malware) on a covered entity’s or business associate’s computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. *See* definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. *See* 45 C.F.R.164.308(a)(6).

63. IBM’s failure to adequately oversee PSC constitutes a violation of HIPAA.

64. IBM was at all times fully aware of its obligation to protect PII. IBM was also aware of the significant repercussions that would result from its failure to do so.

65. Experts studying cyber security routinely identify consumer-facing businesses as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

66. Several best practices have been identified that, at a minimum, should be implemented by services providers such as IBM (and its own third party vendors), including but not limited to: educating all employees about cyber security; requiring strong passwords; maintaining multi-layer security, including firewalls, anti-virus, and anti-malware software; utilizing encryption; making data unreadable without a key; implementing multi-factor authentication; backing up data; and limiting which particular employees can access sensitive data.

67. Other best cybersecurity practices that are standard in the industry include installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; and training staff regarding critical points.

68. These foregoing frameworks are existing and applicable industry standards. IBM failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

***IBM's Breaches of Its Obligations***

69. IBM breached its obligations to Plaintiff and the Class members and was otherwise negligent and/or reckless because it failed to properly maintain, oversee and safeguard its computer systems, network and data, and to oversee its third-party vendors and service providers. In addition to its obligations under federal and state law, IBM owed a duty to Plaintiff and the Class members to exercise reasonable care when obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. IBM owed a duty to Plaintiff and the Class members to provide reasonable security, including complying with industry standards and requirements, training for its staff and ensuring that its computer systems, networks, and protocols adequately protected the PII of Plaintiff and the Class members.

70. IBM's wrongful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

- b. Failing to adequately protect Plaintiff's and the Class members' PII;
- c. Failing to properly monitor third-party data security systems for existing intrusions, brute-force attempts and clearing of event logs;
- d. Failing to ensure that all third-parties apply all available and necessary security updates;
- e. Failing to ensure that all third-parties install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;
- f. Failing to ensure that all third-parties practice the principle of least-privilege and maintain credential hygiene; and failing to avoid the use of domain-wide, admin-level service accounts;
- g. Failing to adequately oversee its own third-party vendors;
- h. Failing to ensure that all third-parties employ or enforce the use of strong randomized, just-in-time local administrator passwords; and
- i. Failing to properly train and supervise third-parties in the proper handling of inbound emails.

71. As the result of these failures, IBM negligently and wrongfully failed to safeguard Plaintiff's and the Class members' PII.

72. Accordingly, as further detailed herein, Plaintiff and Class members now face a substantial, increased, and immediate risk of fraud, identity theft, and the disclosure of their most sensitive and deeply personal information.



***Data Breaches are Disruptive and Harm Victims***

73. The United States Government Accountability Office (“GAO”) released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”

74. That is because all victims of a data breach may be exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it because there is (unfortunately) a market for personally identifiable information, like the PII compromised by the Data Breach.

75. Cybercriminals do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims’ identities in order to engage in illegal financial transactions under the victims’ names. Because a person’s identity is akin to a puzzle, the more accurate individual pieces of data an identity thief obtains regarding a person, the easier it is for that thief to take on the victim’s identity, or otherwise harass or track the victim.

76. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information regarding a victim’s identity, such as a person’s login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

77. The type of information compromised in this Data Breach is even worse than merely a name and date of birth. A stolen Social Security number is a skeleton key to the victim’s identity – and, therefore, the type of data that cyberthieves seek. Identity thieves can use a Social

Security number for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, fraudulently obtaining a job, fraudulently renting a house, or filing a false police report.

78. Because of the threat of these harms, the FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and potentially obtaining an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

79. Theft of PII is gravely serious. PII is an extremely valuable property right.

80. Its value is axiomatic, considering the value of “big data” in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates that PII has considerable market value.

81. According to the GAO:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

*See* GAO Report, at p. 29.

82. Private information, such as the PII compromised herein, is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years. The private information of consumers remains of high value to criminals, as evidenced by the prices paid through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, private information (inclusive of a Social Security number) can be sold at a price from \$40 to \$200, and

bank details have a price range of \$50 to \$200. Experian reports that a stolen credit card or debit card number can sell between \$5 to \$110 on the dark web. Clearly, all this data has real value – which is why it was targeted and stolen in the first place.

83. Additionally, the theft of PHI, in particular, is gravely serious: a thief may use a person's name or health insurance numbers to see a doctor, get prescription drugs, file claims with insurance providers, or get other care. If the thief's health information is mixed with a victim's, the victim's treatment, insurance and payment records, and credit report may be affected.

84. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies also purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

85. Because of the value of the PII compromised in the Data Breach, there is a strong probability that entire batches of information stolen in the Data Breach have been dumped on the black market, as that is the *modus operandi* of cybercriminals who perpetrate data breaches, while other batches have yet to be dumped on the black market, meaning Plaintiff and Class members are at a substantial imminent risk of injury including an increased risk of fraud and identity theft for many years into the future.

86. Thus, Plaintiff and Class members must vigilantly monitor their financial accounts and other indices of identity theft (*i.e.*, the mail, email, etc.) for many years to come.

***Harm to Plaintiff and the Class***

87. On or about August 11, 2023, Plaintiff received notice from HCPF that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that

Plaintiff's PII was compromised as a result of the Data Breach. Plaintiff still has not heard from IBM about the Data Breach.

88. As a result of being informed about the Data Breach (albeit not by IBM), Plaintiff has commenced making reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing reports and her financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff has already spent multiple hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

89. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) actual misuse of her compromised PII; (b) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff; (c) violation of her privacy, including the compromise of highly sensitive PII such as, for example, her Social Security numbers in combination with name and other private information, like PHI; (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud; and (e) actual and potential out-of-pocket losses including the loss of time, as each of the Plaintiff has spent multiple hours dealing with the repercussions of the Data Breach, due to time spent mitigating the actual and potential harms caused by the Data Breach.

## **V. CLASS ALLEGATIONS**

90. Plaintiff brings this nationwide class on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure. The "Nationwide Class" that the Plaintiff seeks to represent is defined as follows:

**Class Definition.** All persons residing in the United States whose PII was maintained by IBM and impacted by the Data Breach.

91. Excluded from the Class are IBM and IBM's subsidiaries, affiliates, officers and directors, and any entity in which IBM has a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

92. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

93. **Numerosity.** HCPF alone (not to mention the many other organizations that hired IBM) reports to the Maine Attorney General that the Data Breach compromised PII of over 4 million individuals. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

94. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

- a. Whether IBM unlawfully used, maintained, lost or disclosed Plaintiff's and the Class members' PII;
- b. Whether IBM failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether IBM's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether IBM's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether IBM owed a duty to Plaintiff and the Class members to safeguard their PII;
- f. Whether IBM breached its duty to Plaintiff and the Class members to safeguard their PII;

- g. Whether computer hackers obtained Plaintiff's and the Class members' PII in the Data Breach;
- h. Whether IBM knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiff and the Class members suffered legally cognizable damages as a result of IBM's misconduct;
- j. Whether IBM's acts, inactions, and practices complained of herein amount to a breach of contract, violations of N.Y. Gen. Bus. Law 349 and/or common law negligence, and whether IBM has been unjustly enriched;
- k. Whether IBM failed to provide notice of the Data Breach, much less in a timely manner; and
- l. Whether Plaintiff and the Class members are entitled to damages, civil penalties, punitive damages, equitable relief and/or injunctive relief.

95. **Typicality.** Plaintiff's claims are typical of those of other Class members because Plaintiff's PII, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiff, like all Class members, was injured by IBM's uniform conduct. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

96. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Class in that they have no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiff suffered are typical of the other Class members, and Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class. Plaintiff has retained counsel experienced in complex class action litigation, including, but not limited to, data privacy class action litigation, and Plaintiff intends to prosecute this action vigorously.

97. **Superiority of Class Action.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class's common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based upon an identical set of facts. Without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

98. The litigation of the claims brought herein is manageable. IBM's uniform conduct, the consistent provisions of the relevant laws and the ascertainable identities of the Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

99. Adequate notice can be given to the Class members directly using information maintained in IBM's records.

100. **Predominance.** The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. IBM engaged in a common course of conduct toward Plaintiff and the Class members. The common issues arising from IBM's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these issues in a single action has important and desirable advantages of judicial economy.

101. This proposed class action does not present any unique management difficulties.

**COUNT I**

**NEGLIGENCE**

102. Plaintiff repeats and re-alleges each and every allegation as if fully set forth herein.

103. Defendant knowingly collected, acquired, stored, and/or maintained Plaintiff's and Class members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting the PII from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

104. The duty included obligations to take reasonable steps to prevent disclosure of the PII, and to safeguard the information from theft. Defendant's duties included the responsibility to design, implement, and monitor data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

105. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the PII.

106. Defendant owed a duty of care to safeguard the PII due to the foreseeable risk of a data breach and the severe consequences that would result from its failure to so safeguard the PII.

107. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and those individuals who (through the corporate and governmental entities to whom they furnished their PII) entrusted IBM with their PII, which special relationship is recognized by laws and regulations including but not limited the FTC Act, HIPAA, as well as common law. Defendant was in a position to ensure that its vendor's



systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and the Class members from a data breach.

108. In addition, Defendant has a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

109. Defendant’s duty to use reasonable care in protecting PII arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect PII that it either acquires, maintains, or stores.

110. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiff’s and the Class Members’ PII, as alleged and discussed above.

111. It was foreseeable that Defendant’s failure to use reasonable measures to protect Class members’ PII would result in injury to Plaintiff and the Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the data transfer and storage industry.

112. It was therefore foreseeable that the failure to adequately safeguard Plaintiff’s and the Class members’ PII would result in one or more types of injuries to Class members.

113. The imposition of a duty of care on Defendant to safeguard the PII they maintained, transferred, stored or otherwise used is appropriate because any social utility of Defendant’s conduct is outweighed by the injuries suffered by Plaintiff and the Class members as a result of the Data Breach.

114. As a direct and proximate result of Defendant’s negligence, Plaintiff and the Class members are at a current and ongoing risk of identity theft, and Plaintiff and the Class members

sustained compensatory damages including: (i) invasion of privacy; (ii) financial “out of pocket” costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iv) financial “out of pocket” costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) diminution of value of their PII; (viii) future costs of identity theft monitoring; (ix) anxiety, annoyance and nuisance, and (x) the continued risk to PII, which remains in Defendant’s and the third-party’s respective control, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff’s and the Class members’ PII.

115. Plaintiff and the Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

116. Defendant’s negligent conduct is ongoing, in that it still holds the PII of Plaintiff and the Class Members in an unsafe and unsecure manner.

117. Plaintiff and the Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

**COUNT II**

**VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349**

118. Plaintiff repeats and re-alleges each and every allegation as if fully set forth herein.

119. New York General Business Law Section 349 (“New York Gen. Bus. Law 349”) prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

120. Defendant is a business as defined by the statute.

121. Plaintiff and the Class members are consumers as defined by the statute.

122. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of New York Gen. Bus. Law 349. The conduct alleged is a “business practice” as defined by the statute, and the deception occurred in New York state.

123. Defendant engaged in deceptive acts or practices in the conduct of business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law 349, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff’s and the Class members’ PII, which was a proximate and direct cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks (including such risks at Defendant’s third-party vendors), remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents involving other organizations, which was a direct and proximate cause of the Data Breach;

- c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and the Class members' PII, including by implementing and maintaining reasonable security measures;
- d. Failing to timely and adequately notify Plaintiff and the Class members of the Data Breach;
- e. Failing to oversee third-party vendors responsible for the storage and transfer of PII;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and the Class members' PII; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the Class members' PII, including duties imposed by the FTC Act, HIPAA and any other applicable statutes.

124. Defendant's representations and omissions regarding data security were material because they were about the critical need and adequacy of Defendant's data security and ability to protect the confidentiality of PII.

125. Defendant acted intentionally and knowingly to violate New York's General Business Law, and recklessly disregarded Plaintiff's and Class members' rights.

126. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and the Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for

fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; and the other harms detailed herein.

127. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large. Defendant's violations of the statute have had an impact on the public, including the people of New York.

128. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and the Class members that they could not reasonably avoid.

129. As such, Plaintiff and the Class members seek statutory damages in the maximum amount allowed per Class member, or, \$50 for each of the millions of victims of the Data Breach. Additionally, Plaintiff and the Class members seek injunctive relief necessary to enjoin further violations and recover costs of this action, including reasonable attorneys' fees and other costs.

### **COUNT III**

#### **UNJUST ENRICHMENT**

130. Plaintiff repeats and re-alleges each and every allegation as if fully set forth herein.

131. Plaintiff and the Class members conferred a monetary benefit on Defendant by providing Defendant with their valuable PII.

132. Defendant enriched itself by saving the costs it reasonably should have expended on data security oversight and other measures to secure Plaintiff's and the Class members' PII, which cost savings increased the profitability of the services.

133. Upon information and belief, instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and the Class members by utilizing cheaper, ineffective security measures. Plaintiff and the Class members, on the other hand, suffered as a direct and

proximate result of Defendant's failure to provide the requisite security by way of third-party vendor(s).

134. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and the Class members.

135. Defendant acquired the monetary benefit, PII, through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

136. Had Plaintiff and the Class members known that Defendant had not adequately secured their PII, they would not have agreed to provide their PII to the corporate and governmental entities (such as HCPF) that, in turn, hired Defendant. Plaintiff and the Class members have no adequate remedy at law.

137. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class members have suffered and will continue to suffer other forms of injury and/or harm.

138. Furthermore, as a direct and proximate result of Defendant's ineffective, unreasonable and inadequate data security practices, Plaintiff and the Class members are at a current and ongoing risk of identity theft and have sustained incidental and consequential damages, including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their PII; (vii) future costs of identity theft monitoring; and (viii) the continued risk to their PII, which remains in Defendant's and third-party control, and which is subject to further breaches, so long as Defendant

fails to undertake appropriate and adequate measures to protect Plaintiff's and the Class members' PII.

139. Plaintiff and the Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

140. Plaintiff and the Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

141. Moreover, Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and the Class members, proceeds that it unjustly received from them.

#### **COUNT IV**

#### **DECLARATORY JUDGMENT**

142. Plaintiff repeats and re-alleges each and every allegation as if fully set forth herein.

143. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state laws and regulations described in this Complaint.

144. Defendant owes a duty of care to Plaintiff and the Class members, which required it to adequately secure and oversee the protection of Plaintiff and the Class members' PII.

145. Defendant still possesses the PII of Plaintiff and the Class members.

146. Defendant's data security measures remain inadequate. Furthermore, Plaintiff and the Class members continue to suffer injury as a result of the compromise of their PII and the risk remains that further compromises of their PII will occur in the future.

147. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Defendant owes a legal duty to secure its victims' PII and to timely notify victims of the Data Breach;
- b. Defendant's existing data security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect PII; and
- c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure and oversee the protection of victims' PII.

148. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect victims' PII, including the following:

- a. Order Defendant to provide a lifetime of credit monitoring and identity theft insurance to Plaintiff and the Class members.
- b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:
  - i. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks,



- penetration tests, and audits on Defendant's systems (and its third-party vendors' systems on a periodic basis;
- ii. ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
  - iii. engaging third-party security auditors and internal personnel to run automated security monitoring;
  - iv. auditing, testing, and training its security personnel regarding any new or modified procedures;
  - v. conducting regular database scanning and security checks;
  - vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs (either internally or at a third-party vendor) and what to do in response to such a breach; and
  - vii. meaningfully educating its end-users about the threats they face with regard to the security of their PII as well as the steps those users should take to protect themselves.

149. If an injunction is not issued, Plaintiff and the Class members will suffer irreparable injury and will lack adequate legal remedy to prevent another data breach. The risk of another such breach is real, immediate, and substantial. If another breach of Defendant's or third-party systems occurs, Plaintiff and the Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

150. The hardship to Plaintiff and the Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiff and the Class members will

likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligations to employ such measures.

151. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendant, thus preventing future injury to Plaintiff and the Class members whose PII would be further compromised.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on her own behalf and on behalf of all others similarly situated, pray for relief as follows:

- A. For an Order certifying this case as a class action, appointing Plaintiff as the lead plaintiff in this Action, and appointing Plaintiff's below-listed counsel as lead counsel of this Action;
- B. For an award of restitution, actual damages, compensatory damages, statutory damages, nominal damages and statutory penalties, in an amount to be determined, as allowable by law;
- C. For an award of equitable and injunctive relief;
- D. For injunctive and other equitable relief to ensure the protection of the sensitive information of Plaintiff and the Class members which remains in Defendant's possession;
- E. For an award of attorneys' fees and costs;
- F. For pre- and post-judgment interest on any amounts awarded; and

G. For such other and further relief as the Court may deem just and proper.

**JURY TRIAL DEMAND**

152. Plaintiff hereby demands a trial by jury of all claims so triable.

**DATED:** August 30, 2023

Respectfully submitted,

/s/ Israel David

Israel David

Blake Hunter Yagman

Madeline Sheffield

**ISRAEL DAVID LLC**

17 State Street, Suite 4010

New York, New York 10004

Tel.: 212-739-0622

Fax: 212-739-0628

Email: *israel.david@davidllc.com*

*blake.yagman@davidllc.com*

*madeline.sheffield@davidllc.com*

*Attorneys for Plaintiff and the Class*